# ZAŠTITA I BEZBEDNOST INFORMACIJA
## ISPITNA PITANJA 2010/2011

1. Šta je bezednost računarskog sistema?
2. Zbog čega je važno upravljanje sigurnošću informacija?
3. Kojim pretnjama mogu biti izloženi informacioni resursi?
4. Kakve pretnje bi trebalo uzeti u obzir kada je u pitanju sistem komuniciranja?
5. Šta se podrazumeva pod terminom sigurnosni menadžment?
6. Šta se podrazumeva pod upravljanjem sigurnošću informacija?
7. Koji su osnovni ciljevi upravljanja sigurnošću informacija?
8. Šta je raspoloživost informatičkih resursa?
9. Šta je poverljivost informatičkih resursa?
10. Šta je integritet informatičkih resursa?
11. Šta je rizik i kako se računa?
12. Koje su osnovne kategorije napada na računarske sisteme?
13. Šta je kontrola pristupa u kontekstu sigurnosti informacija?
14. Podela kontrole pristupa na osnovu ciljeva.
15. Podela kontrole pristupa na osnovu mera primene.
16. Šta je administrativna kontrola pristupa?
17. Šta je tehnička kontrola pristupa?
18. Šta je fizička kontorla pristupa?
19. Osnovni servisi kontrole pristupa.
20. Provera identiteta.
21. Lozinka.
22. Biometrija.
23. Tokeni.
24. Metodologija kontrole pristupa.
25. Metodi napada u računarski sistem.
26. Podela kontrola pristupa prema obaveznosti.
27. Zašto se pored zakonske regulative i tehničkih mehanizama za upravljanje sigurnošću informacija insistira i na primenu odgovarajućih standarda, kao priznatih modela za upravljanje sigurnošću informacija?
28. Kako se može izvršiti podela standarda za upravljanje sigurnošću informacija prema području primene i prema nameni?
29. Zbog čega bi standard ISO 17799 trebalo dati prednost u odnosu na ostale standarde za upravljanje sigurnošću informacija?
30. Koje mere sigurnosti definiše standard ISO/IEC 17799:2000?
    a. navesti i detaljnije objasniti.
31. Standardi ISO/IEC 27001 i ISO/IEC 27002:
    a. odnos
    b. istorijat
32. Ciljevi standarda ISO/IEC 27001:2005?
33. Primena PDCA krug prema ISO 27001.
34. Na osnovu kojih standarda i zahteva se izrađuje dokumentacija Sistema za upravljanje sigurnošću informacija i šta bi sve trebalo da sadrži?
35. Kako je raspoređena osnovna propisana dokumentacija na piramidi dokumentacije Sistema za upravljanje sigurnošću informacija?
36. Šta mora da sadrži politika sigurnosti?

37. Šta je priručnik sigurnosti?
38. Šta je Registar informatičkih resursa?
39. Šta se podrazumeva pod upravljanjem dokumentima?
40. Šta je to audit i u čemu se ogleda značenje proveravanja Sistema za upravljanje sigurnošću informacija?
41. Kakvi auditi postoje, s obzirom na klijente?
42. Šta je osnovna svrha dokumentacionog audita sistema za upravljanje sigurnošću informacija?
43. Šta je osnovna svrha implementacionog audita sistema za upravljanje sigurnošću informacija?
44. Koje aktivnosti bi trebalo sprovesti tokom audita?
45. Kakvi mogu da budu rezultati audita?
46. Kakva je uloga država u funkciji zaštite informatičkih resursa?
47. Istorijat pravne zaštite informacija.
48. Šta je kompjuterski kriminalitet?
49. Šta je kompjuterska krađa?
50. Šta je kompjuterska prevara?
51. Šta je kriminal vezan za kompjuterske mreže?
52. Cyber kriminal.
53. Posledice kompjuterskog kriminala.
54. Kompjuterski terorizam
55. Značaj međunarodne saradnje na pravnoj zaštiti sigurnosti informacija?
56. Navesti krivična dela protiv bezbednosti računarskih podataka (KZRS, 2005, Gl.27)
57. Navesti krivična dela protiv intelektualne svojine (KZRS, 2005, Gl. 20)
58. Podela softvera prema zakonskom obliku zaštite
59. Doktrina poštenog korišćenja
60. Kada možete imati poverenje u sopstvene informacije?
61. Kriptografija
62. Šta je elektronski (digitalni) potpis
63. Digitalni sertifikat
64. Steganografija
65. Osnovni elementi za stvaranje on-line poverenja
66. Kako se etika uklapa u kontekstu ostvarivanja sigurnosti informacija?
67. Značaj kulture sigurnosti informacija kada je u pitanju elektronsko poslovanje?
68. Kakve pretnje sigurnosti informacija dolaze od zaposlenih?
69. Šta je to protivpravno korišćenje usluga i neovlašćeno pribavljanje informacija?
70. Socijalni inženjering
71. Zbog čega je važno gajiti kulturu sigurnosti informacija?
72. Kako se mogu neutralisati unutrašnje pretnje?
73. Testiranje zaštite (Etičko hakerisanje)
74. Etički kodeks Instituta za kompjutersku etiku
75. Zlonamerni softver (definicija i podela)
76. Trojanski konji (trojanci)
77. Crvi
78. Virusi
79. Špijunski programi (spyware)
80. DOS (Denial-of-Service (DoS) napad
81. Bot mreža
82. Hoaxes (obmana)
83. Zaštita od zlonamernog softvera

Predmetni nastavnik:
dr Ana Kovačević

Literatura:


1. Milan Kukrika: *Upravljanje sigurnošću informacija – Zaštita informacionih sistema prema standardu ISO 17799*, INFO Home, Beograd, 2002.
2. Ana Kovačević, Slajdovi sa predavanja, Fakultet bezbednosti, 2010.


Beograd, 17.12.2010.